PART4　情報セキュリティ

目標
- 情報セキュリティについて理解する。
- 身の回りの情報セキュリティを確保する方法について考えることができるようになる。

Chapter1　情報セキュリティ

情報セキュリティの３要素

情報セキュリティとは，機密情報の流出やデータの改ざん・破壊などが起こらないように，〔①　　　　　〕，〔②　　　　　〕，〔③　　　　　〕などの観点から対策を講じることである。

情報セキュリティは，情報の〔④　　　　　　〕・〔⑤　　　　　　〕・〔⑥　　　　　　〕を維持することが重要である。これを，情報セキュリティの３要素という。

機密性
Confidentiality
許可された人，もしくは権利を持った人だけが情報にアクセスできる状態のこと

完全性
Integrity
第三者に不正に情報を書き換えられたり，破壊されたりしない状態のこと

可用性
Availability
情報を使いたいときにいつでもアクセスできる状態のこと

ファイアウォール

- **ファイアウォールの種類**

〔⑦　　　　　　　　　　〕：ネットワークの通信において，その通信を許可するかどうかを判断し，許可または拒否する仕組み。

知っておこう
ファイアウォールは，「通過させる通信」「通過させない通信」のルールの設定が必要になる。ルール設定を誤ると，正常な通信を遮断したり，不正な通信を通過させたり，誤検知を発生させたりする可能性がある。設定したルールが問題ないかを定期的に確認することが大切である。

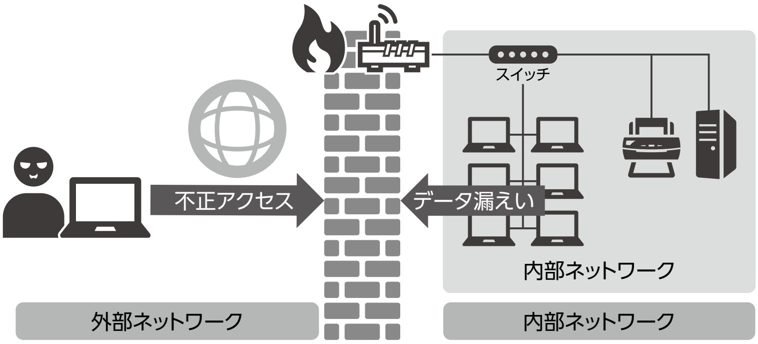
ファイアウォールには，次のような種類がある。

• **パーソナルファイアウォール**

主に〔⑧　　　　　　〕のコンピュータを対象とし，外部ネットワークからの侵入やコンピュータ内部からの外部ネットワークへの通信を検知，遮断を目的とするファイアウォール。

• **企業ネットワーク等のファイアウォール**

インターネットとLAN（内部ネットワーク）の間に設置し，外部からの〔⑨　　　　　　〕を防いだり，内部からの〔⑩　　　　　　〕を防いだりする目的のファイアウォール。



コンテンツフィルタリング

• **コンテンツフィルタリング**

コンテンツフィルタリングとは，好ましくないWebサイトやサービスの閲覧，利用を制限する仕組みのことである。代表的なフィルタリング方式に，〔⑪　　　　　　　　　　〕と〔⑫　　　　　　　　　　〕がある。

• **ブラックリスト方式**

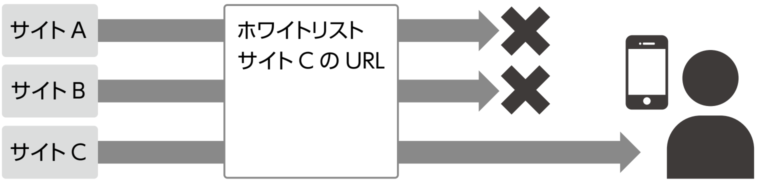
ブラックリスト方式は，不適切なサイトの一覧を作成し，そのリストのサイトを見せなくする方式のことである。

知っておこう

フィルタリングのリストは，サイトのURLを定義する方法のほか，特定のキーワードを定義し，そのキーワードが含まれるサイトを閲覧できなくする方法などもある。

• ホワイトリスト方式

ホワイトリスト方式は，安全で有益なサイトの一覧を作成し，そのリストに存在するサイトだけ閲覧可能とする方式のことである。



無線LANのセキュリティ

無線 LAN は電波を使って通信しているため，強固なセキュリティをかける必要がある。セキュリティホールが見つかるたびに，暗号化方式は進化を遂げている。以下は無線 LAN の暗号化の歴史である。

	暗号化規格	主な暗号化方式	暗号化強度
1997 年～	〔⑬ 〕	WEP	弱
2002 年～	〔⑭ 〕	TKIP（暗号キーを毎回変更)	↓
2004 年～	WPA2	CCMP(暗号化アルゴリズム AES)	↓
2018 年～	WPA3	CCMP(暗号化アルゴリズム AES/CNSA)	強

知っておこう

WEP（Wired Equivalent Privacy)
WPA（Wi-Fi Protected Access)
TKIP（Temporal Key Integrity Protocol)
CCMP（Counter mode with CBC-MAC Protocol)
AES(Advanced Encryption Standard)
CNSA(Commercial National Security Algorithm)

まとめ

- 情報セキュリティの３要素は,「**機密性**」「**完全性**」「**可用性**」で，これらを維持することが重要である。
- **ファイアウォール**は，ネットワークの通信において，その通信を許可するかどうかを判断し，許可または拒否する仕組みのことである。
- **コンテンツフィルタリング**は，好ましくない Web サイトやサービスの閲覧・利用を制限する仕組みのことである。
- 無線 LAN は電波を用いて通信しているため，利用時は特にセキュリティに注意しなければならない。

Chapter2　実践問題

問１　次のア～ウの説明について，「機密性」「完全性」「可用性」の３要素から，最も関連のあるものを答えなさい。

ア　テレビ番組で商品紹介があるので，アクセスが集中してWebサーバがダウンしないように，あらかじめサーバの増強を行った。

イ　学校の内申書のデータには，担当する先生だけがアクセスできるようにしている。

ウ　データの改ざんや破壊などの被害を防ぐため，定期的にバックアップを取得している。

問２　次の会話はケンジ君とハナコさんが，情報セキュリティについて授業で学んだ内容を語り合う場面の会話である。しかし，この会話内には１つ誤りがある。何が誤っているかを答えなさい。

ケンジ：ファイアウォールについて興味を持ったからネットで調べたんだけど，名前の由来は，火災のときに被害を最小限に食い止める「防火壁」から来ているんだって！

ハナコ：さすがケンジ君。授業で学んだことを更に掘り下げて調べるなんて素敵！ファイアウォールがあれば，どんな不正なアクセスが来ても食い止められるから一度導入すれば安心だね。

ケンジ：やっぱり情報っておもしろいね！

問３　Web サイトの閲覧を制限するために，コンテンツフィルタリングを導入することにした。ホワイトリスト方式で以下の様にサイト URL のリストを定義した。閲覧できるサイトおよび閲覧できないサイトは，それぞれどのようなものか，50 字程度で説明しなさい。

【ホワイトリスト】
サイト A の URL
サイト B の URL

問４　次のア～エの無線 LAN セキュリティの説明について，正しければ○，誤っていれば×を答えなさい。

ア　現在主流の暗号化規格は WEP である。

イ　暗号化規格 WPA3 の主な暗号方式は，CCMP（楕円曲線暗号）である。

ウ　WEP → WPA → WPA2 → WPA3 の順でセキュリティ強度は弱くなる。

エ　公衆無線 LAN などで複数の暗号化規格が選択可能な場合は，できるだけ強固なものを選択する。

第8講　PART4　確認問題

問 1　機密情報の流出やデータの改ざん・破壊などが起こらないように，個人，組織，技術などの観点から対策を講じる必要がある。情報セキュリティの３要素とは，a 機密性，b 完全性，c 可用性のことである。

(1)　下線部 a に関する文章として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　業務用のパソコンにパスワードでロックをかけている
②　情報管理システムのサーバを複数台で分散運用している
③　データの編集後は上書き保存して，ファイルを増やさないようにしている
④　データの編集履歴を残すシステムを採用している

(2)　下線部 b に関する文章として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　業務用のパソコンにパスワードでロックをかけている
②　情報管理システムのサーバを複数台で分散運用している
③　データの編集後は上書き保存して，ファイルを増やさないようにしている
④　データの編集履歴を残すシステムを採用している

(3)　下線部 c に関する文章として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　業務用のパソコンにパスワードでロックをかけている
②　情報管理システムのサーバを複数台で分散運用している
③　データの編集後は上書き保存して，ファイルを増やさないようにしている
④　データの編集履歴を残すシステムを採用している

問2 ファイアウォールに関する説明として最も適切なものを，次の①～④のうちから選びなさい。

① 外部からの侵入を防ぐために，通信が発生しない間はインターネットとの接続を解除している

② 外部からのアクセスをすべて遮断している

③ 企業などのネットワークでは，インターネットとLANの間に設置して，セキュリティを向上を図っている

④ 正常な通信と不正な通信は，設定したルールに則れば必ず見分けることができる

問3 ある学校では，aブラックリストの特徴を考慮し，校内のネット閲覧にコンテンツフィルタリングを行うことにした。ブラックリストとして次のリストを用意した。

【ブラックリスト】
サイトA・サイトB・サイトD

(1) 閲覧可能なサイトを，次の①～④のうちから一つ選びなさい。

① サイトA	② サイトB
③ サイトC	④ サイトD

(2) 下線部aについて述べた文章として最も適切なものを，次の①～④の中から一つ選びなさい。

① 一度設定すれば，リストの見直しなどのメンテナンスは不要というメリットがある

② 管理者が知らない不適切なサイトを生徒が閲覧できてしまう可能性はあるが，広く情報を集めることができる

③ 管理者が知らない有益なサイトを生徒は閲覧できないが，想定したサイトを確実に表示させることができる

④ 閲覧可能なサイトの一覧なので生徒はサイトを安全に閲覧できる

第8講　情報通信ネットワーク

PART1　ネットワーク

問1　（ア）②　（イ）④　（ウ）①　（エ）③

問2　（ア）サーバ　（イ）クライアント　（ウ）サーバ

問3　省略

PART2　プロトコル

問1　（ア）②　（イ）①　（ウ）④　（エ）③

問2　IPアドレスはドットを境に8ビット単位なので，10進法では0～255の範囲となる。よって，258の部分はあり得ない数値である。

問3　（ア）×　UDPは再送制御を行わない。

（イ）×　双方に互換性がないことから，まだIPv6への移行途中の段階。

（ウ）×　ルータのルーティングによって，それぞれのパケットごとに違う経路の場合もある。

PART3　WWWとメール

問1　④→②→③→①

問2　（ア）×　（イ）×　（ウ）○　（エ）×

問3　（ア）SMTP　（イ）SMTP　（ウ）POP

問4　「ドメイン名は,DNSサーバの住所」の部分が誤り。この会話でのドメイン名は,DNSサーバの住所ではなくWebサーバの住所が正しい。

PART4　情報セキュリティ

問1　（ア）可用性　（イ）機密性　（ウ）完全性

問2　ファイアウォールで食い止められない不正アクセスも多々あり，定期的なルールの見直しも必要である。

問3　サイトAおよびサイトBは閲覧できるが，それ以外のサイトの閲覧はフィルタリングルールにより拒否される。

問4　（ア）×　（イ）○　（ウ）×　（エ）○

PART5　暗号化とデジタル署名

問１　（ア）公開鍵暗号方式　（イ）共通鍵暗号方式

（ウ）共通鍵暗号方式　（エ）共通鍵暗号方式

問２　（ア）公開鍵　（イ）秘密鍵

問３　（ア）○

（イ）×　ハッシュ値から，元のメッセージを推測することは困難である。

（ウ）×　元のメッセージが１文字でも異なれば, 全く異なるハッシュ値となる。

（エ）○

問４　（ア）○

（イ）×　共通鍵を受け渡すための鍵交換には公開鍵暗号方式を使い，その後のやり取りするデータの暗号化には，公開鍵暗号方式より高速な共通鍵暗号方式を用いるのが正しい。

（ウ）○

（エ）×　URL が「http:// ～」の場合は，通信経路が暗号化されていない。

PART6　情報システムとデータベース

問１　ウ

問２　（ア）C to C　（イ）B to C　（ウ）B to B

問３　（ア）○　（イ）○　（ウ）×　（エ）○

PART7　データベース管理システム

問１　（ア）×　（イ）○　（ウ）○　（エ）×

問２　（ア）③　（イ）①　（ウ）②

問３　（ア）①，②，③　（イ）①，②　（ウ）①

第 8 講 PART4　確認題　解答

問 1

(1) ①

解説：
機密性とは，特定の利用者のみがアクセスできる状態のことである。

(2) ④

解説：
完全性とは第三者によってシステムやデータなどが破壊されることがない状態のことである。

(3) ②

解説：
可用性とは，いつでもシステムやデータに安全にアクセスできる状態のことである。

問 2　③

解説：
ファイアウォールは，ネットワークの通信において，セキュリティ上の問題のある通信かどうかを判断し，許可・拒否する仕組みである。その判断基準は，利用者が設定することができる。

問 3

(1) ③

解説：
ブラックリスト方式では，この例の場合，サイトＣにアクセスすることができる。

(2) ②

解説：
ブラックリストに載っていないサイトにはアクセスできる点に注意が必要である。